**What Do You Mean – I Can't Have Copies of the Medical Records I Need For Trial?**

By Lisa L. Dahm, J.D., LL.M. Candidate
lldahm@earthlink.net

Ask a non-attorney what the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] is, and a likely response will be that it is a law protecting the confidentiality of patients' medical records. Ask an attorney what HIPAA is, and one response may be that it is a law used by healthcare providers to avoid having to respond to attorneys' requests for medical records and other health information. Although healthcare providers may seem uncooperative in response to attorney-issued subpoenas, the providers may just be concerned about complying with the detailed authorization requirements set forth in the final privacy regulations which were promulgated to help assure the success of administrative simplification (the Privacy Regulations).[2]

The general rule under the Privacy Regulations is that covered entities[3] may not use or disclose an individual's protected health information (PHI)[4] for purposes unrelated to treatment, payment, healthcare operations, or certain defined exceptions[5] without first obtaining the individual's prior written authorization.[6] Although covered entities may use and disclose PHI for "legal services"[7] and for certain judicial and administrative proceedings[8] without first obtaining the individual's prior authorization, a covered entity may not disclose PHI to an attorney in response to a subpoena without additional "satisfactory assurances."[9]

Covered healthcare providers that do not receive such satisfactory assurances must obtain a valid authorization before disclosing PHI to an attorney.[10] Under the

Privacy Regulations, a valid authorization must contain all of the following elements and statements:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion. For example, "medical records maintained by Dr. A relating to patient X created between September 1, 2002, and December 31, 2002."

- The name of the person or entity authorized to make the requested disclosure. For example, "Dr. A's office" or "Community Medical Center Hospital."

- The name of the person or entity to whom the covered entity will make the disclosure. If a records service is obtaining copies of medical records on behalf of an attorney, the authorization should identify the records service as the organization to which the disclosure should be made or the attorney should enclose with the records service's request a letter indicating that the records service is working on the attorney's behalf.

- A description of each purpose of the requested disclosure. The statement of purpose must be sufficiently specific to place the patient on notice of each of the purposes for the disclosure. The statement "for the purpose of litigation" may not provide the patient whose records are being requested with sufficient notice as contemplated by the Privacy Regulations. However, the statement, "For the purpose of representing Patient A in the lawsuit resulting from the automobile accident that occurred in January 2005" would be sufficient.

- An expiration date or event that relates to the individual or the purpose of the use or disclosure.

- Signature of the individual and date. If the authorization is signed by a personal representative of the individual, a description of the representative's authority to act for the individual must also be provided.

- A statement that the patient has the right to revoke the authorization at any time in writing and the exceptions to the right to revoke.

- A statement regarding the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization.

- A statement regarding the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by the Privacy Regulations.[11]

Because all of these elements and statements must be included in each authorization form, some covered healthcare providers prefer not to release PHI unless the patient has signed the provider's own authorization form. These providers usually have recognized that: (1) the authorization accompanying the attorney's request may not contain all of the required elements and statements; (2) it would take too long to review and revise each authorization form presented by each attorney requesting medical records; (3) the civil and criminal sanctions set forth in HIPAA for inappropriate disclosures of healthcare information apply only to covered healthcare providers, not attorneys;[12] and (4) state laws that allow patients to recover for improper information disclosures generally only allow recovery from the healthcare entity that made the improper disclosure.[13] Attorneys who are familiar with which healthcare providers require use of their own authorizations may wish to obtain extra copies of and use such authorizations in order to prevent situations in which the patient must return to the attorney's office to execute more than one authorization for the same set of records.

Although the Privacy Regulations do not directly apply to attorneys, they do affect the ability of attorneys to obtain medical records for use in litigation. In light of the Privacy Regulations' detailed requirements relating to authorizations, today's litigators may be forced to use authorizations created by healthcare providers. However, attorneys who are willing to use these authorizations may have an easier time obtaining the desired records, and will be helping to strike the appropriate balance between patient confidentiality and legitimate use of health information for legal purposes.

[1] Pub. L. No. 104-191 (Aug. 21, 1996), *codified at* 42 U.S.C. § 1320d *et seq*.
[2] In the Administrative Simplification Subtitle of HIPAA, Congress established six standards to govern the electronic communication of health information within and between healthcare entities. *See* 42 U.S.C. § 1320d-2. In enacting HIPAA, Congress recognized that administrative simplification would not work without some assurance that the privacy and confidentiality of the electronically communicated health information could be guaranteed. Congress empowered the Department of Health and Human Services (HHS) to adopt regulations governing the privacy of individually identifiable health information in the event Congress was unable to pass comprehensive federal privacy legislation within three years of HIPAA's enactment. Pub. L. No. 104-191, § 264(c)(1). The final regulations were published on December 28, 2000, and were amended on August 14, 2002. *See* 65 Fed.Reg. at 82,462-82,829 (Dec. 28, 2000), *amended by* 67 Fed. Reg. 53182 (Aug. 14, 2002) (codified at 45 C.F.R. Parts 160, 164). All covered entities, except small health plans, were required to comply with the HIPAA Privacy Regulations by April 14, 2003. 45 C.F.R. § 164.534.
[3] Covered entities are defined to include health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form in connection with a standard HIPAA transaction. *Id.* § 160.103.
[4] Protected health information is individually identifiable health information. *Id*. § 164.501.
[5] *See id.* §§ 164.506, 164.512.
[6] *Id*. § 164.508.
[7] *Id.* § 164.506(c)(1) (permitting a covered entity to use and disclose PHI for its own health care operations without prior authorization); *id*. § 164.501 (defining health care operations to include legal services). The combination of these two regulatory provisions would permit, for example, a defendant physician to use or disclose patient information to defend him or herself without obtaining the prior written authorization of the patient who is the subject of the information.
[8] *Id*. § 164.512(e)(1)(ii).
[9] *Id.* A covered entity receives "satisfactory assurances" if it receives a written statement and supporting documentation that the individual whose health information is being sought has been notified of the subpoena and has been given an opportunity to contest the subpoena. *Id.* §§ 164.512(e)(1)(iii) and (iv).
[10] *Id*. § 164.508.
[11] *Id*. § 164.508(c)(1) and (2).
[12] A covered entity that violates the Privacy Regulations may incur civil fines of $100 per violation, up to a maximum of $25,000 per year, as well as criminal penalties that range from a fine of $50,000 and/or one year in prison up to a fine of $250,000 and/or ten years in prison. *See* 42 U.S.C. §§ 1320d-5, 1320d-6.
[13] For example, section 241.156 of the Texas Health & Safety Code provides, "the patient has a cause of action against a healthcare provider who makes an unauthorized disclosure of health information." If it is the patient's physician who improperly discloses the patient's health information, the patient is entitled to file for an injunction or a lawsuit for damages. *See* TEX. OCC. CODE ANN. §159.009. *See also*, LISA L. DAHM, 50-STATE SURVEY ON PATIENT HEALTH CARE RECORD CONFIDENTIALITY (American Health Lawyers Association Expert Series, 1999).